

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-173892

(43)Date of publication of application : 13.07.1993

(51)Int.Cl.

G06F 12/14
G06F 9/445
G06F 9/06
G06F 12/14

(21)Application number : 03-345124

(71)Applicant : NEC CORP

(22)Date of filing : 26.12.1991

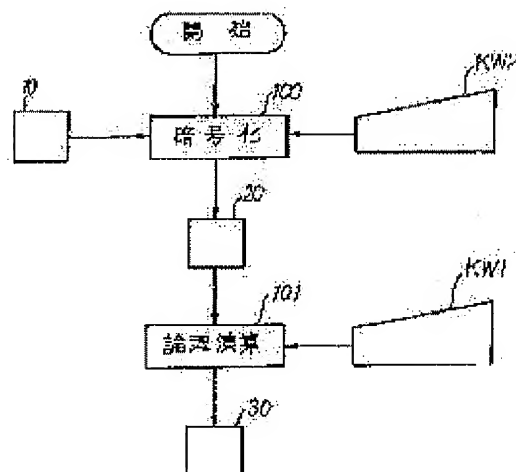
(72)Inventor : KOMATSU HIROYOSHI

(54) FILE LOADING SYSTEM

(57)Abstract:

PURPOSE: To obtain a file loading system where the alternation of the load module file of an execution type and the illegal operation of a computer are prevented.

CONSTITUTION: A first logical operation processing is executed in a file 20 which is obtained by ciphering the load module file 10 so as to generate a check digit, the check digit is added to a ciphering file 20 so as to form a ciphering file 30 with the check digit and it is inputted to the computer. The computer executes the second operation processing by the same rule as the first logical operation to the inputted file 30, compares the operation result with the check digit, refuses a loading when both does not coincide and decodes a ciphering file part so as to execute the loading when they coincide.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-173892

(43)公開日 平成5年(1993)7月13日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0 B	9293-5B		
9/445				
9/06	4 5 0 B	8944-5B		
12/14	3 1 0 Z	9293-5B		
		8944-5B		
			G 0 6 F 9/ 06	4 2 0 A
			審査請求 未請求 請求項の数 2(全 4 頁)	

(21)出願番号 特願平3-345124

(22)出願日 平成3年(1991)12月26日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 小松 寛佳

東京都港区芝五丁目7番1号 日本電気株式会社社内

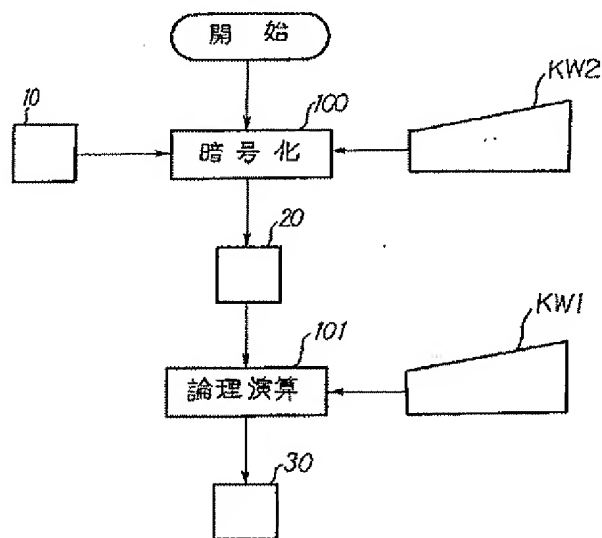
(74)代理人 弁理士 後藤 洋介 (外2名)

(54)【発明の名称】 ファイルロード方式

(57)【要約】

【目的】 実行形式のロードモジュールファイルの改ざんや、コンピュータの不正動作を防止するファイルロード方式を提供する。

【構成】 ロードモジュールファイル10を暗号化したファイル20に第一の論理演算処理を施してチェックデジットを生成し、このチェックデジットを暗号化ファイル20に付加してチェックデジット付暗号化ファイル30を形成し、これをコンピュータ(図示省略)に入力する。コンピュータでは、入力されたファイル30に第一の論理演算と同一法則による第二の演算処理を施してその演算結果と前記チェックデジットとを比較し、両者不一致のときはロードを拒否する一方、一致のときは暗号化ファイル部分を復号化してロードを行う。



【特許請求の範囲】

【請求項1】 実行形式のロードモジュールファイルを情報処理装置にロードするファイルロード方式において、

前記ロードモジュールファイルを暗号化したファイルに第一の論理演算処理を施してチェックデジットを生成し、このチェックデジットを前記暗号化したファイルに付加してチェックデジット付暗号化ファイルを形成した後、このチェックデジット付暗号化ファイルの暗号化ファイル部分に前記第一の論理演算と同一法則による第二の演算処理を施し、その演算結果と前記チェックデジットとを比較して、両者不一致のときは情報処理装置へのロードを拒否し、一致のときは暗号化ファイル部分を復号化して情報処理装置へのロードを行うことを特徴とするファイルロード方式。

【請求項2】 前記ロードモジュールファイルの暗号化と前記暗号化ファイル部分の復号化の際、及び、前記第一の論理演算処理と前記第二の論理演算処理の際に、夫々同一のキーワードを設定し、これらキーワードが夫々一致したときのみ前記情報処理装置へのロードを行い得るようにしたことを特徴とする請求項1記載のファイルロード方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、コンピュータ等の情報処理装置（以下コンピュータと称する）に実行形式のプログラム格納ファイルをロードする方式に関する。

【0002】

【従来の技術】 従来、コンピュータにプログラムをロードするときは、プログラム開発者が実行形式のプログラムロードモジュールファイルを作成し、そのファイルをそのままコンピュータにロードしていた。

【0003】

【発明が解決しようとする課題】 しかしながら、このようなロード方式では、プログラム開発者以外の者が容易にそのプログラムを改ざんし、改ざんしたプログラムをロードしてコンピュータを不正に動作させることが可能となる問題があった。

【0004】 また、プログラムのロードモジュールより逆アセンブルしてそのプログラム内容を第三者に知られてしまう問題があった。

【0005】 本発明はかかる問題点を解決することを目的とする。

【0006】

【課題を解決するための手段】 本発明は、上記目的を達成するため、実行形式のロードモジュールファイルを情報処理装置にロードするファイルロード方式において、前記ロードモジュールファイルを暗号化したファイルに第一の論理演算処理を施してチェックデジットを生成し、このチェックデジットを前記暗号化したファイルに

付加してチェックデジット付暗号化ファイルを形成した後、このチェックデジット付暗号化ファイルの暗号化ファイル部分に前記第一の論理演算と同一法則による第二の演算処理を施し、その演算結果と前記チェックデジットとを比較して、両者不一致のときは情報処理装置へのロードを拒否し、一致のときは暗号化ファイル部分を復号化して情報処理装置へのロードを行うようにした。

【0007】

【実施例】 以下、図面を参照して本発明の実施例を説明する。

【0008】 まず、暗号化ロードモジュールファイルを形成する手順を、図1のフローチャートを参照して説明する。

【0009】 プログラムデバッグを終了したロードモジュールファイル10を第二のキーワードデータKW2とともに暗号化処理し（ステップ100）、暗号化ロードモジュールファイル20を作成する。暗号化の方式に関しては様々な方式が考案されているが、本実施例ではその方式を問わない。

【0010】 この暗号化ロードモジュールファイル20は第一のキーワードデータKW1により一定の法則に従った第一の論理演算処理を施してチェックデジットを生成し（ステップ101）、このチェックデジットを暗号化ロードモジュールファイル20に付加してチェックデジット付暗号化ロードモジュールファイル30を形成する。チェックデジットを生成する方式に関してもモジュラス10、モジュラス11等様々な方式が考案されているが、本実施例では特に問わない。

【0011】 次に、このようにして形成されたチェックデジット付暗号化ロードモジュールファイル30をコンピュータ（図示省略）にロードする時の手順を図2のフローチャートを参照して説明する。

【0012】 まず、第一のキーワードデータKW1とチェックデジット付暗号化ロードモジュールファイル30とを図1の論理演算処理（ステップ101）と同一法則による第二の論理演算処理を施し（ステップ102）、その演算結果をチェックデジット付暗号化ロードモジュールファイル30に付加されているチェックデジットと比較する（ステップ103）。

【0013】 その結果、不一致の場合はアラームを表示して処理を終了させ（ステップ106）、一致する場合には第二のキーワードデータKW2とチェックデジット付暗号化ロードモジュールファイル30とを図1の暗号化処理と同一法則により復号化し（ステップ104）、復号化されたロードモジュールファイルをコンピュータのメモリに展開する（ステップ105）。

【0014】 なお、図1に示す第一のキーワードデータKW1と図2に示す第一のキーワードデータKW1とは全く同一のものであり、図1に示す第二のキーワードデータKW2と図2に示す第二のキーワードデータKW2も全く同

10

20

30

40

50

一のものである。

【0015】

【発明の効果】以上説明したように、本発明は、実行形式のロードモジュールファイルを暗号化するとともに、暗号化されたロードモジュールファイルに第一の論理演算処理を施してチェックデジットを生成し、このチェックデジットを暗号化ファイルに付加するようにしたので、プログラム内容の第三者による解読が不可能になる。

【0016】また、コンピュータでは、入力されたファイルの第二の論理演算処理によりファイル内容の同一性を判定し、同一性が確認されたときのみ暗号化ファイルを復号化し、その内容をメモリに展開するようにしたので、プログラム内容が改ざんされてプログラムが不正に動作されることが防止されるという効果を有する。

【0017】更に、暗号化と復号化、及び、第一の論理演算処理と第二の論理演算処理に夫々同一のキーワード*

*を設定し、これらキーワードが一致したときのみ暗号化ファイルを復号するようにしたので、上記効果がより顕著になる。

【図面の簡単な説明】

【図1】本発明の一実施例に係るファイルロード方式を実行するための暗号化ロードモジュールファイルを形成する手順を示すフローチャートである。

【図2】本実施例により形成されたチェックデジット付暗号化ロードモジュールファイルをコンピュータにロードする時の手順を示すフローチャートである。

【符号の説明】

10 ロードモジュールファイル

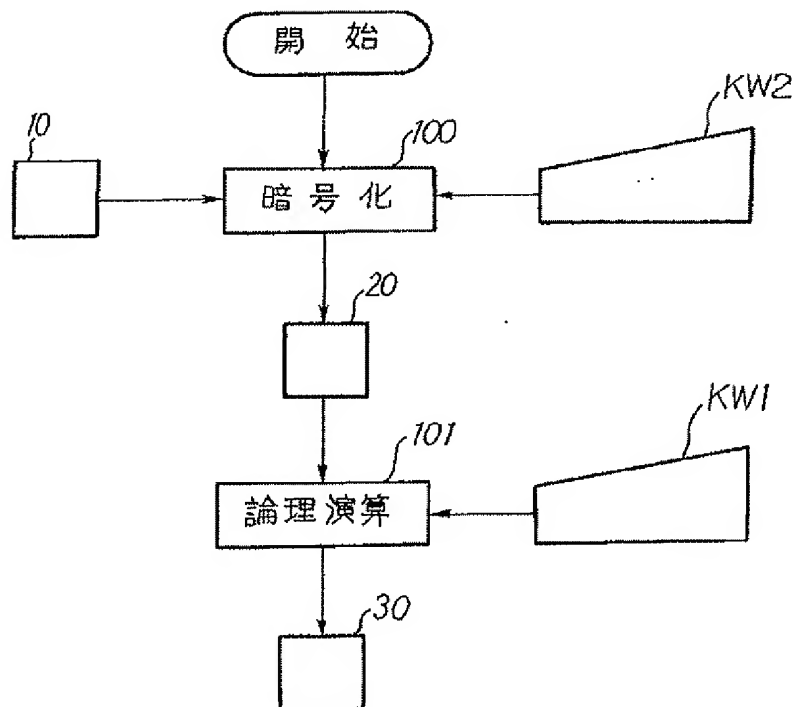
20 暗号化ロードモジュールファイル

30 チェックデジット付暗号化ロードモジュールファイル

KW1 第一のキーワード

KW2 第二のキーワード

【図1】



【図2】

